RINGS

Recall: An ideal I is a subset of ring R such that

i) $(I,+)$ is a subgroup of R.

ii) For $r \in R$, $s \in I$, $rs \in I$.

Examples:

$$\{0\} \subset R$$

$$R \subset R$$

$$n\mathbb{Z} \subseteq \mathbb{Z}$$

$$\langle x \rangle \subseteq \mathbb{Z}[x]$$

$$\| $$

$$\{ x f(x) \mid f(x) \in \mathbb{Z}[x] \}$$

or in general

$$\langle g(x) \rangle \subseteq \mathbb{Z}[x]$$

Qn: What are all the ideals of $\mathbb{Q}$? $\mathbb{R}$?

Defn: Let $S = \{r_1, r_2, \ldots, r_n\} \subset R$. We say that I is an <u>ideal generated by S</u> if $I = \{r_1 x_1 + r_2 x_2 + \cdots + r_n x_n \mid x_i \in R\}$

Lemma: I is an <u>ideal generated by S</u>

$$\iff I = \bigcap_{\substack{J \text{ ideal} \\ S \subseteq J}} J$$

Pf: $\Rightarrow$: Suppose J is an ideal that contains S.

$$\Rightarrow I \subseteq J$$

$$\Rightarrow I \subseteq \bigcap_{\substack{J \text{ ideal} \\ S \subseteq J}} J$$

$S \subseteq I$, so $\displaystyle\bigcap_{\substack{J \text{ ideal} \\ S \subseteq J}} J \subseteq I$

$$\Rightarrow I = \bigcap_{\substack{J \text{ ideal} \\ S \subseteq J}} J$$

$\Leftarrow$ Assume $I = \bigcap_{\substack{J \text{ ideal} \\ S \subseteq J}} J$

We want to show that

$$I = \{r_1x_1 + r_2x_2 + \cdots + r_nx_n \mid x_i \in R\}$$

Consider $\{r_1x_1 + r_2x_2 + \cdots + r_nx_n \mid x_i \in R\}$, it is an ideal, contains S so, contains I.

$$\{r_1x_1 + r_2x_2 + \cdots + r_nx_n \mid x_i \in R\} \subseteq I$$

Hence, shown.

If $S = \{r\}$, we say that the ideal generated by S is principal.

<u>Examples:</u> In $\mathbb{Z}$ and $\mathbb{Z}[x]$, every ideal is principal.

Quotient Rings

A natural thing to do would be to take a subring S of R and take

$$R/S = \text{set of cosets of } S$$
$$= \{ r + S \mid r \in R \}$$

and define addition & multiplication as follows

$$(r_1 + S) + (r_2 + S) = (r_1 + r_2) + S$$

This is well defined because if

$$r_1 + S = r_1' + S \iff r_1 - r_1' \in S$$

and $r_2 + S = r_2' + S \iff r_2 - r_2' \in S$

then $(r_1 + r_2) - (r_1' + r_2') \in S$

$$\iff (r_1 + r_2) + S = (r_1' + r_2') + S$$

$$(r_1+S)(r_2+S) = (r_1 r_2) + S$$

If $r_1 - r_1' \in S$

$r_2 - r_2' \in S$

then $(r_1 - r_1')(r_2 - r_2') \in S$

but this does not necessarily imply that $r_1 r_2 - r_1' r_2' \in S$

Example: $\mathbb{Z} \subseteq \mathbb{Q}$ is a subring

$\mathbb{Q}/\mathbb{Z}$

Consider cosets $\frac{1}{2} + \mathbb{Z}$ and $\frac{1}{3} + \mathbb{Z}$

$$\frac{1}{2} + \mathbb{Z} = \frac{3}{2} + \mathbb{Z} \qquad \frac{1}{3} + \mathbb{Z} = \frac{4}{3} + \mathbb{Z}$$

but $\frac{1}{6} + \mathbb{Z} \neq \frac{12}{6} + \mathbb{Z}$

So, multiplication is not well-defined.

Suppose instead we take quotient by an ideal.

R/I

$$r_1 + I = r_1' + I \iff r_1 - r_1' \in I$$

$$r_2 + I = r_2' + I \iff r_2 - r_2' \in I$$

then $$r_1 r_2 - r_1' r_2' = r_2 \underbrace{(r_1 - r_1')}_{\in I} + r_1' \underbrace{(r_2 - r_2')}_{\in I}$$

So, R/I has both addition & multiplication defined on it.

It is a ring, also known as quotient ring.

Examples: 1) $n\mathbb{Z} \subseteq \mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ is a ring.

2) $R/R = \{0\}$

$R/\{0\} = R$

3) $\langle x \rangle \subseteq \mathbb{Z}[x]$

$$\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$$

$$\mathbb{Z}[x]/\langle x^2+1 \rangle \cong \mathbb{Z} \times (x\mathbb{Z})$$

RING HOMOMORPHISMS

Defn: Let R_1, R_2 be two rings.

A map $\phi: R_1 \to R_2$ is a ring homomorphism

if (1) $\phi(a+b) = \phi(a) + \phi(b)$

(2) $\phi(ab) = \phi(a)\,\phi(b)$

(3) $\phi(1) = 1$

Examples: 1) $\mathbb{Z} \to \mathbb{Z}$

$n \mapsto n$

2) $\mathbb{Z}[x] \to \mathbb{Z}[x]$

$n \in \mathbb{Z} \mapsto n$

$x \mapsto x^2$

3) $\mathbb{Z} \to R$

$1 \mapsto 1$

$n \mapsto n \cdot 1$

4) $R \to R/I$

$a \mapsto a + I$

$\varphi: R_1 \to R_2$ ring homomorphism

$\ker \varphi = \{ a \in R_1 \mid \varphi(a) = 0 \}$

<u>Lemma:</u> $\ker \varphi$ is an ideal of R_1.

<u>pf:</u> It is a subgroup of R_1, with respect to addition.

Suppose $a \in \ker \varphi$, $r \in R_1$, then

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)\,0 = 0$$

Image $\varphi = \{ \varphi(a) \mid a \in R_1 \}$

<u>Lemma:</u> Image φ is a subring of R_2.

<u>pf:</u> It is a subgroup with respect to addition, contains 0 and 1.

If $x, y \in$ Image φ

$x = \varphi(a)$ $\quad y = \varphi(b)$, then

$$xy = \varphi(a)\,\varphi(b) = \varphi(ab)$$

So $xy \in$ Image φ.

Examples: 1) $\mathbb{Z} \to \mathbb{Z}$

$$n \mapsto n$$

$\ker = \{0\}$ Image $= \mathbb{Z}$

2) $\mathbb{Z}[x] \to \mathbb{Z}[x]$

$$n \mapsto n$$

$$x \mapsto x^2$$

If $\varphi(f) = 0$

$$\varphi(a_0 + a_1 x + \cdots + a_n x^n) = 0$$

$$a_0 + a_1 x^2 + a_2 x^4 + \cdots + a_n x^{2n} = 0$$

$$\Rightarrow a_i = 0$$

$$f = 0$$

$\ker = \{0\}$

Image $= \mathbb{Z}[x^2]$

3) $\mathbb{Z} \longrightarrow R$

$n \longmapsto n \cdot 1$

$\ker = (\operatorname{char} R)\,\mathbb{Z}$

$$\begin{array}{ccc} & \text{Image} & \\ {\scriptstyle \operatorname{char} R = 0} \swarrow & & \searrow {\scriptstyle \operatorname{char} R = n} \\ \mathbb{Z} & & \mathbb{Z}/n\mathbb{Z} \end{array}$$

4) $R \longrightarrow R/I$

$a \longmapsto a+I$

$\ker = \{ a \mid a+I = I \}$

$= I$

$\text{Image} = R/I$

<u>Defn:</u> A <u>ring isomorphism</u> is a ring homomorphism that is bijective on underlying sets.

FIRST ISOMORPHISM THEOREM

$\varphi : R_1 \to R_2$ ring homomorphism

$$R_1 / \mathrm{Ker}\,\varphi \cong \mathrm{Image}\ \varphi$$

$\downarrow$

Ring isomorphism